AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A machine implemented method of monitoring traffic flow in a monitoring device disposed to receive network traffic packets, the method comprising: ~~comprises:~~

producing statistics corresponding to a parameter of traffic flow to trace the source of an attack, with producing further comprising:

mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets;

accumulating statistics from the packets; and

comparing the number of buckets to a threshold; and

determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold.

2. (Allowed) The method of claim 1 wherein the buckets are storage areas in a memory space of the monitor device.

3. (Allowed) The method of claim 1 wherein as the number of buckets changes, the buckets have values derived from the buckets prior to the change.

4. (Allowed) The method of claim 1 wherein the hash function adapts to map to the new number of buckets, as the new number of buckets changes.

5. (Allowed) The method of claim 1 wherein comparing statistic values comprises:

comparing the value accumulated in the bucket to a threshold that depends on the number of buckets.

6. (Allowed) The method of claim 1 wherein the parameter is the count of how many packets a data collector or gateway examines.

7. (Allowed) The method of claim 1 wherein as a value of a parameter for one bucket approaches a threshold, the monitoring device raises an alarm.

8. (Allowed) The method of claim 1 wherein the hash function changes periodically in a randomly secret manner so that packets are reassigned to different buckets.

9. (Allowed) The method of claim 1 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored, so that the monitoring device is not vulnerable to a denial of service attack against its own resources.

10. (Allowed) The method of claim 1 wherein the variable number of buckets efficiently identifies the source or sources of attack by breaking down traffic into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in each bucket.

11. (Allowed) The method of claim 1 wherein the traffic is monitored at multiple levels of granularity, from aggregate to individual flows.

12. (Allowed) The method of claim 1 wherein the method is applied to monitoring of TCP packet ratios and repressor traffic.

13. (Allowed) The method of claim 1 wherein the threshold is a first threshold and the method further comprises:

comparing accumulated statistic values from the buckets to second threshold values to determine that an event is of significance.

14. (Currently Amended) A computer program product residing on a computer readable storage medium for monitoring network traffic flow in a network, the computer program product comprising ~~comprises~~ instructions for causing a computer to:

map traffic flow into a plurality of buckets by applying a hash function "f(h)" to a parameter of the traffic flow to output an integer corresponding to one of the buckets;

accumulate statistics from the packets; and

compare the accumulated statistic values from the buckets to configured threshold values corresponding to the number of buckets to determine that an event is of significance; and

adjust the number of buckets as the number of buckets approaches a second threshold.

15. (Allowed) The computer program product of claim 14 wherein based on the second threshold, the buckets are divided into more buckets or combined into fewer buckets

16. (Allowed) The computer program product of claim 14 wherein instructions to monitor further comprise instructions to

divide the bucket into a different number of new buckets containing values derived from the original bucket.

17. (Allowed) The computer program product of claim 14 wherein the hash function adapts to map to the new number of buckets as the new number of buckets changes.

18. (Allowed) The computer program product of claim 14 wherein the parameter is the count of how many packets a data collector or gateway examines.

19. (Allowed) The computer program product of claim 14 wherein the buckets are storage areas in the memory space of the monitor device.

20. (Allowed) The computer program product of claim 14 wherein the hash function changes periodically in a randomly secret manner so that packets are reassigned to different buckets.

21. (Currently Amended) A data collector to collect statistical information about network flows ~~comprises~~ comprising:

a computer readable medium;

a computing device that executes a computer program product stored on the computer readable medium comprising instructions to cause the computing device to:

map traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets;

accumulate statistics from the packets; and

compare the accumulated statistic values from the buckets to configured threshold values corresponding to the number of buckets to determine that an event is of significance; and

adjust the number of buckets as the number of buckets approaches a second threshold.

22-49 (Cancelled)

50. (Allowed) The data collector of claim 21 wherein based on the second threshold, the buckets are divided into more buckets or combined into fewer buckets

51. (Allowed) The data collector of claim 21 wherein instructions to monitor further comprise instructions to

divide the bucket into a different number of new buckets containing values derived from the original bucket.

52. (Allowed) The data collector of claim 21, wherein the hash function adapts to map to the new number of buckets as the new number of buckets changes.

53. (Allowed) The data collector of claim 21 wherein the parameter is the count of how many packets the data collector examines.

54. (Allowed) The data collector of claim 21 wherein the buckets are storage areas in the memory space of the monitor device.

55. (Allowed) The data collector of claim 21 wherein the hash function changes periodically in a randomly secret manner so that packets are reassigned to different buckets.

56. (Allowed) The data collector of claim 21 wherein instructions to compare statistic values comprises instructions to:

compare the value accumulated in the bucket to a threshold that depends on the number of buckets.

57. (Allowed) The data collector of claim 21 wherein as a value of a parameter for one bucket approaches a threshold, the monitoring device raises an alarm.

58. (Allowed) The data collector of claim 21 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored, so that the data collector is not vulnerable to a denial of service attack against its own resources.

59. (Allowed) The data collector of claim 21 wherein the variable number of buckets efficiently identifies the source or sources of attack by breaking down traffic into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in each bucket.

60. (Allowed) The data collector of claim 21 wherein the traffic is monitored at multiple levels of granularity, from aggregate to individual flows.

61. (Allowed) The data collector of claim 21 wherein the traffic is applied to monitoring of TCP packet ratios and repressor traffic.

62. (Allowed) The data collector of claim 21 wherein the threshold is a first threshold and the computer program further comprises instructions to:

compare accumulated statistic values from the buckets to second threshold values to determine that an event is of significance.

63. (Allowed) A method of monitoring traffic flow in a monitor device disposed to receive network traffic packets comprises:

producing statistics corresponding to a parameter of traffic flow to trace the source of an attack, with producing further comprising:

mapping the traffic flow into a plurality of buckets;

varying the number of buckets according to the amount of traffic and number of flows according to down traffic flow into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in the bucket.

64. (Allowed) The method of claim 63 wherein varying varies the number of buckets so that the monitoring device is not vulnerable to DoS attacks against its own resources.

65. (Allowed) The method of claim 63 wherein varying the number of buckets comprises:

comparing the number of buckets to a threshold number of buckets;

determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold and as the number of buckets changes, the buckets have values derived from the buckets prior to the change.

66. (Allowed) The method of claim 63 wherein further comprising:

comparing accumulated statistic values from the buckets to second threshold values to determine that an event is of significance.

67. (Allowed) The method of claim 63 wherein comparing statistic values comprises:

accumulating statistic values from the packets; and

comparing the values accumulated in the buckets to thresholds that depend on the number of buckets.

68. (Allowed) The method of claim 63 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored, so that the monitoring device is not vulnerable to a denial of service attack against its own resources.

69. (Allowed) The method of claim 63 wherein the buckets are storage areas in a memory space of the monitor device and mapping the traffic flow into a plurality of buckets comprises:

applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets.

70. (Allowed) A computer program product residing on a computer readable medium for monitoring traffic flow in a monitor device disposed to receive network traffic packets comprises instructions for causing the device to:

produce statistics corresponding to a parameter of traffic flow to trace the source of an attack, with producing further comprising:

map the traffic flow into a plurality of buckets;

vary the number of buckets according to the amount of traffic and number of flows according to down traffic flow into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in the bucket.

71. (Allowed) The computer program product of claim 70 wherein instructions to vary, vary the number of buckets so that the monitoring device is not vulnerable to DoS attacks against its own resources.

72. (Allowed) The computer program product of claim 70 wherein instructions to vary comprises instructions to:

compare the number of buckets to a threshold number of buckets;

determine whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold and as the number of buckets changes, the buckets have values derived from the buckets prior to the change.

73. (Allowed) The computer program product of claim 70 further comprising instructions to:

compare accumulated statistic values from the buckets to second threshold values to determine that an event is of significance.

74. (Allowed) The computer program product of claim 70 wherein instructions to compare statistic values' comprises instructions to:

accumulate statistic values from the packets; and

compare the values accumulated in the buckets to thresholds that depend on the number of buckets.

75. (Allowed) The computer program product of claim 70 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored, so that the monitoring device is not vulnerable to a denial of service attack against its own resources.

76. (Allowed) The computer program product of claim 70 wherein the buckets are storage areas in a memory space of the monitor device and instructions to map the traffic flow into a plurality of buckets comprises instructions to:

apply a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets.

77. (Allowed) The data collector of claim 21 further comprising:

a port to link the data collector to a central control center.